



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/854,666	05/15/2001	Kaoru Uchida	Q64528	1139

7590 10/01/2004

SUGHRUE, MION, ZINN, MACPEAK & SEAS
2100 Pennsylvania Avenue, N.W.
Washington, DC 20037-3202

EXAMINER

TRAN, ELLEN C

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 10/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/854,666

Applicant(s)

UCHIDA, KAORU

Examiner

Ellen C Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 May 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-29 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-29 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 19 Jul 2001.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: original application filed 10 May 2001, with acknowledgement of foreign application date of 31 May 2000. *gm*
2. Claims 1-29 are currently pending in this application. Claims 1, 22, 23, and 24 are independent claims.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

4. **Claims 1-4, 9, 10, 20-24, and 26-29** are rejected under 35 U.S.C. 102(e) as being anticipated by Musgrave et al. U.S. Patent No. 6,202,151 (hereinafter '151).

As to independent claim 1, “An identification system comprising: a plurality of end terminals” is taught in '151 col. 4, lines 23-24 (i.e. “plurality of end terminals” same as “set of input devices”)

“each of the end terminals transmitting a transaction request message containing biometrics data of a user and a user identifier of said user to a communications network; at least one electronic commerce service provider (ECSP) unit” is shown in '151 col. 4, lines 53-60 (i.e. “electronic commerce service provider (ECSP)” same as “entity such as corporation”)

“for receiving said transaction request message via said network and transmitting an authentication request message containing said biometrics data and said user identifier to said network” is disclosed in ‘151 col. 3, lines 40-48;

“and an authentication server having a database for mapping a plurality of registered biometrics data to a plurality of corresponding registered user identifiers, the authentication server receiving the authentication request message via said network comparing the received biometrics data to one of the registered biometrics data which is mapped in said database to the user identifier contained in said authentication request message and returning a reply to said ECSP unit via said network indicating that said transaction request message is authenticated if the received biometrics data coincides with said mapped biometrics data” is taught in ‘151 col. 5, lines 36-67.

As to dependent claim 2, **“wherein each of said end terminals is configured to cipher the biometrics data so that the biometrics data contained in said transaction request message and said authentication request message is the ciphered biometrics data, and wherein said authentication server is configured to decipher the ciphered biometrics data contained in the received authentication request message”** is shown in ‘151 col. 4, line 53 through col. 5, line 27.

As to dependent claim 3, **“wherein said ECSP unit includes a conversion table for mapping a first plurality of user identifiers to a second plurality of user identifiers, wherein said first plurality of user identifiers are used by said plurality of end terminals and said second plurality of user identifiers are the user identifiers registered in said database, said ECSP unit converting the user identifier contained in the received transaction request**

message to one of the second plurality of user identifiers which is mapped to the received user identifier and transmitting said authentication request message containing the converted user identifier” is disclosed in ‘151 col. 5, line 53 through col. 6, line 12.

As to dependent claim 4, “wherein each of said end terminals is configured to cipher the biometrics data with a secret key generated by a variable secret key generator which generates secret keys which vary with time, the generated secret key being agreed-upon with said authentication server” is taught in ‘151 col. 5, lines 27-35.

As to dependent claim 9, “wherein said biometrics data of said user is a fingerprint of said user” is shown in ‘151 col. 4, lines 30-33.

As to dependent claim 10, “wherein said biometrics data of said user is an extracted feature of a fingerprint of said user” is disclosed in ‘151 col. 5, lines 6-11.

As to independent claim 20, “An identification method comprising the steps of: a) transmitting, from an end terminal a transaction request message containing biometrics data of a user to a communications network” is taught in ‘151 col. 4, lines 53-60;

“b) receiving at an electronic commerce service provider, said transaction request message via said network” is shown in ‘151 col. 3, lines 40-48;

“c) transmitting, from the electronic commerce service provider, an authentication request message containing said biometrics data to said network; d) receiving said authentication request message via said network at a user authenticator having a database for storing a plurality of registered biometrics data; e) determining whether the received biometrics data has corresponding biometrics data in said database; and f) returning a reply from said user authenticator to said electronic commerce service provider via said

network indicating that said transaction request message is authenticated if the received biometrics data coincides with one of the registered biometrics data of the database” is disclosed in ‘151 col. 5, lines 36-67.

As to dependent claim 21, “wherein the step (a) further comprises ciphering the biometrics data and transmitting said transaction request message containing the ciphered biometrics data to said network, and wherein the step (d) further comprises the step of deciphering the biometrics data contained in the received authentication request message” is shown in ‘151 col. 4, line 53 through col. 5, line 27.

As to independent claim 22, “An identification method comprising the steps of: a) transmitting, from an end terminal, a transaction request message containing biometrics data of a user and a user identifier of said user to a communications network” is disclosed in ‘151 col. 4, lines 53-60;

“b) receiving, at an electronic commerce service provider, said transaction request message via said network” is taught in ‘151 col. 3, lines 40-48;

“c) transmitting, from the electronic commerce service provider, an authentication request message containing said biometrics data and said user identifier to said network; d) receiving said authentication request message at a user authenticator via said network, the authenticator having a database in which a plurality of registered biometrics data are mapped to a plurality of corresponding registered user identifiers; e) comparing the received biometrics data to one of the registered biometrics data which is mapped in said database to the user identifier contained in said authentication request message; and f) returning, from the user authenticator, a reply to said electronic commerce service

provider via said network indicating that said transaction request message is authenticated if the received biometrics data coincides with said mapped biometrics data” is shown in ‘151 col. 5, lines 36-67.

As to dependent claim 23, “wherein the user identifiers stored in said database are different from the user identifiers of said end terminals, further comprising converting, at said service provider, the user identifier contained in the received transaction request message to a second user identifier which is contained in said authentication request message as the first-mentioned user identifier” is disclosed in ‘151 col. 5, line 53 through col. 6, line 12.

As to dependent claim 24, “wherein the step (a) further comprises ciphering the biometrics data and transmitting said transaction request message containing the ciphered biometrics data to said network, and wherein the step (d) further comprises the step of deciphering the biometrics data contained in the received authentication request message” is taught in ‘151 col. 4, line 53 through col. 5, line 27.

As to independent claim 26, “An identification method comprising the steps of: a) transmitting, from an end terminal, a transaction request message containing biometrics data of a user to a communications network” is shown in ‘151 col. 4, lines 53-60;

“b) receiving, at an electronic commerce service provider, said transaction request message via said network” is disclosed in ‘151 col. 3, lines 40-48;

“c) transmitting from said service provider, an authentication request message containing said biometrics data to said network; d) receiving, at a user authenticator having a database in which a plurality of registered biometrics data are mapped to a

Art Unit: 2134

plurality of corresponding registered user identifiers, said authentication request message via said network; e) comparing the received biometrics data to all of the registered biometrics data in said database to detect coincidence; f) detecting the user identifier mapped to the biometrics data which coincides with the received biometrics data; and g) returning a reply from the user authenticator to said service provider via said network indicating that said user having the detected user identifier is authenticated” is taught in ‘151 col. 5, lines 36-67.

As to dependent claim 27, **“wherein the step (a) further comprises ciphering the biometrics data and transmitting said transaction request message containing the ciphered biometrics data to said network, and wherein the step (d) further comprises the step of deciphering the biometrics data contained in the received authentication request message”** is shown in ‘151 col. 4, line 53 through col. 5, line 27.

As to independent claim 28, **“An identification system comprising: a plurality of end terminals”** is taught in ‘151 col. 4, lines 23-24;

“each of the end terminals transmitting to a communications network a registration request message and a transaction request message, each of said messages containing biometrics data of a user and a user identifier of said user at least one electronic commerce service provider (ECSP) unit” is shown in ‘151 col. 4, lines 53-60;

“for receiving said registration request message via said network to retransmitting the registration request message to said network and receiving said transaction request message via said network” is disclosed in ‘151 col. 3, lines 40-48;

“and transmitting an authentication request message containing said biometrics data and said user identifier to said network; and an authentication server for receiving said registration request message from said ECSP unit via said network, mapping in a database a plurality of biometrics data contained in a plurality of said registration request messages to a plurality of corresponding user identifiers contained in said registration request messages, the authentication server further receiving the authentication request message via said network, comparing the received biometrics data to one of the biometrics data which is mapped in said database to the user identifier contained in said authentication request message and returning a reply to said ECSP unit via said network indicating that said transaction request message is authenticated if the received biometrics data coincides with said mapped biometrics data” is taught in ‘151 col. 5, lines 36-67.

As to independent claim 29, **“An identification system comprising: a plurality of end terminals”** is taught in ‘151 col. 4, lines 23-24;

“each of the end terminals transmitting a registration request message containing biometrics data of a user and a user identifier of the user to a communications network and transmitting a transaction request message containing said biometrics data to the communications network; at least one electronic commerce service provider (ECSP) unit” is shown in ‘151 col. 4, lines 53-60;

“for receiving said registration request message via said network and retransmitting the registration request message to said network and receiving said transaction request message and transmitting an authentication request message containing said biometrics data to said network; and an authentication server for receiving

Art Unit: 2134

said registration request message from said ECSP unit via said network” is disclosed in ‘151 col. 3, lines 40-48;

“mapping a plurality of biometrics data contained in a plurality of said registration request messages to a plurality of corresponding user identifiers contained in said registration request messages, the authentication server receiving the authentication request message via said network, comparing the received biometrics data to all of the biometrics data in said database, detecting the user identifier mapped to the biometrics data which coincides with the received biometrics data, and returning a reply to said ECSP unit via said network indicating that a user identified by the detected user identifier is authenticated” is taught in ‘151 col. 5, lines 36-67.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. **Claims 5-8, and 25** are rejected under 35 U.S.C. 103(a) as being unpatentable over ‘151 as applied to claims above in further view of Glass et al. U.S. Patent No. 6,332,193 (hereinafter ‘193).

As to dependent claim 5, the following is not taught in '151 **“wherein said variable secret key generator is located at said authentication server and wherein each of said end terminals is configured to transmit a key request message to said authentication server via said ECSP unit to receive said secret key from the secret key generator and ciphering the biometrics data with the received secret key before said transaction request message is transmitted”** however '193 shows “Referring to FIG. 7 the transaction begins when the client system 1 requests access to a resource protected by the server computer 10. For example, an individual wishes to use his computer 2 to access the money transfer screens that enable him to move funds from his bank account to another account. This could be a transfer from his savings account to his checking account or a payment of bills by sending funds to the account of one of his vendors. The authentication server 10 has a request handler 12 which receives the inquiry. Upon receiving the request the authentication server computer 10 initiates a security transaction to ultimately provide access to the protected resource. The server, as part of the transaction, generates a unique token or set of unique tokens, one of which is sent back to the client. The tokens are created by a token generator 13 and may be generated as a result of a random number generator, a random key generator, a unique transaction number, a time stamp, or a combination of any or all of the above” in col. 9, lines 15-25.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '151 a technique for combining biometric identification to authenticate a user identity to include a means to prevent the biometric information from being altered. One of ordinary skill in the art would have been motivated to perform such a

modification to prevent attackers from impersonating an identity. As indicated by '193 (see col. 2, lines 13 et seq.) "There are several key places where an attacker could perform this image substitution ... Thus, there is a need for a method and device which can transmit biometric data while preventing image substitution or tampering".

As to dependent claim 6, "wherein said authentication server comprises a variable secret key generator which generates a secret key which varies with time, and a description unit for deciphering the received ciphered biometrics data by using the secret key generated by said secret key generator" is taught in '193 col. 7, line 33 through col. 8, line 13 "If a token scheme is used, the token is generated by the server 10 and communicated to the client system 1 just prior to image capture ... the server can set a clock which causes tokens to expire after some period of time. In fact, a clock expiration scheme does not need tokens to work; as long as the transaction can be timed and there is a finite window of opportunity for the client to send an image back to the server, some protection is offered ... However, a time stamp may be included in the algorithm for generating the token, or the token itself may be some representation of time ... Another possible variation of the implementation of the token scheme involves generating unique values which function as keys for a digital signature algorithm which uses a key or keys. This is slightly different than an implementation in which the token generator merely generates unique blocks of data, since the token generator must generate unique, but valid, keys. This also offers the ability to use an asymmetric digital signature algorithm ... For an asymmetric algorithm, two tokens or keys are generated. The first key is sent to the camera, and the second or complementary key is kept within the server. The latter method provides additional security since one key never leaves the secure server".

As to dependent claim 7, “wherein each of said end terminals comprises a user terminal exclusively owned by said use” is shown in ‘193 col. 4, lines 6-10 “The secret key assures that an attacker with knowledge of the image, token and code generation algorithm cannot create a valid code for a substituted or tampered image. The secret key may be a serial number or other identification number that is unique to the camera or sensor that collects the biometric data. If such a code is used we can provide a separate camera certification authority which contains a listing of authorized cameras”

As to dependent claim 8, “wherein each of said end terminals comprises a sales terminal to which a plurality of user's handheld personal units can be connected, wherein said sales terminal transparently transmits a transaction request messaged received from each of the personal units to said ECSP unit” is disclosed in ‘193 col. 8, lines 22-45 “FIG. 6 shows how client and server systems would be connected together In FIG. 6 there are several client systems 1a, 1b through 1n. Each client system has a host computer 2 and associated imaging system 4 which includes a camera. The client systems can be connected to one of many authentication servers systems 10a, 10b through 10n. Theses servers may be associated with other computer systems that perform online banking transactions. Other authentication servers may be associated with other vendors whose services or products may be purchased over the network 9. This network most likely will be the Internet but it could be another public carrier such as a telephone system or satellite transmission system. When the selected server receives a request for access from on of the clients it sends a query for one of the keys, the public key, to a central Camera Certification Authority 30, which would hold all public keys for all cameras. The inquiry contains the serial number reported by the camera. The public key would be used to

Art Unit: 2134

determine whether a particular camera signed the image received by the server using that same camera's internal private key" (i.e. "sales terminals" same as "vendor"/ "handheld" same as "satellite transmission systems")

As to dependent claim 25, "wherein the biometrics data contained in the transaction request message is ciphered by using a secret key which varies with time and agrees with the secret key with which the ciphered biometrics data is deciphered at said user authenticator" is taught in '193 col. 7, line 33 through col. 8, line 13.

7. **Claims 11-19** are rejected under 35 U.S.C. 103(a) as being unpatentable over '151 in further view of '193.

As to independent claim 11, "An identification system comprising: a plurality of end terminals" is taught in '151 col. 4, lines 23-24 "The disclosed biometric certification system 24 is shown in FIGS 3-4. It has a set of input devices";

"each of the end terminals transmitting a transaction request message containing biometrics data of a user to a communications network; at least one electronic commerce service provider (ECSP) unit" is shown in '151 col. 4, lines 53-60 "The biometric certificate as shown in FIG. 2 may be generated by concatenating transaction data, public key, and the set 16 of data, including the biometric data 20, using a first concatenator 32 ... corresponding to the electronic transaction such as an electronic funds transfer. The set 16 of data is input through the user data input device 28 which may be in a sequence, as "

“for receiving said transaction request message via said network and transmitting an authentication request message containing said biometrics data to said network” is disclosed in ‘151 col. 3, lines 40-48 “A receiver responds to the data signal received from the network and operates to extract the digital biometric certificate signal”;

“and an authentication server having a database for mapping a plurality of registered biometrics data to a plurality of corresponding registered user identifiers, the authentication server receiving the authentication request message via said network, comparing the received biometrics data to all of the registered biometrics data in said database, detecting the user identifier mapped to the biometrics data which coincides with the received biometrics data, and retuning a reply to said ECSP unit via said network indicating that a user identified by the detected user identifier is authenticated” is taught in ‘151 col. 5, lines 36-67 “after receiving the electronic transaction from the network 42, a receiver 44 decrypts the electronic transaction using its private key, de-hashes the hash function 34, and extracts the biometric certificate 46 ... The receiver 44, then sends the biometric certificate to a biometric certificate management system (BCMS) for authentication thereof ... The BCMS 48 also accesses a biometric database 54 to obtain pre-stored biometric data from registered users identified by the user data ... The classifier 52 may be a comparator, or alternatively a software routine .. data matching techniques, for comparing the biometric data to obtain a decision value”.

the following is not taught in ‘151: **“respectively identified by user identifiers”** however ‘193 teaches “When the selected server receives a request for access from on of the clients it sends a query for one of the keys, the public key, to a central Camera Certification Authority 30, which

would hold all public keys for all cameras. The inquiry contain the serial number reported by the camera. The public key would be used to determine whether a particular camera signed the image received by the server using that same camera's internal private key" in col. 8, lines 33-40.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '151 a technique for combining biometric identification to authenticate a user identity to include a means to prevent the biometric information from being altered. One of ordinary skill in the art would have been motivated to perform such a modification to prevent attackers from impersonating an identity. As indicated by '193 (see col. 2, lines 13 et seq.) "There are several key places where an attacker could perform this image substitution ... Thus, there is a need for a method and device which can transmit biometric data while preventing image substitution or tampering".

As to dependent claims 12-19, these claims contain substantially similar subject matter as dependent claims 2, and 4-19 above and are therefore rejected along similar rationale.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Glaze et al.	U.S. Patent No. 6,320,970	issued 11/20/2001
Hoffman et al.	U.S. Patent No. 5,613,012	issued 03/18/1997
Nozato Katsuji	JP Patent No. 11-338947	issued 10/12/1999

Art Unit: 2134

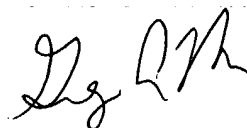
9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (703) 305-8917. **"After 26 October 2004, the examiner can be reach at (571) 272-3842".**

The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
16 September 2004



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100